HP IMAGING AND PRINTING SECURITY CENTER 2.0

Frequently Asked Questions

CONTENTS

Introduction 2
Installation 3
Policy 3
Devices 4
Assess & Remediate 6
Reports 7
Instant-On Security 9

INTRODUCTION

This document provides answers to frequently asked questions about the HP Imaging and Printing Security Center 2.0 release.

INSTALLATION

Q. How can I identify all of the local instances of SQL during IPSC installation?

A. If all of the local instances of SQL do not appear in the IPSC database selection window during the installation process, you can usually retrieve SQL instance information by executing SQL Configuration Manager and selecting SQL Server Services.

Q. Why am I having trouble connecting to a local instance of SQL Server 2012?

A. Beginning with SQL Server 2012, database engine security enhancements now include provisioning during setup, new property list permissions, new user-defined server roles and new ways of managing server and database roles. These changes were implemented by Microsoft to provide greater security at install time. IPSC installation is not exempt from this enhanced security. So, unless the IPSC installer is granted SQL Server Administrator rights during SQL Server 2012 setup, the installer must be provided **sysadmin** rights later and before IPSC is installed with the option to utilize a local instance of SQL Server 2012.

Q. Why is the Microsoft Report Viewer installed during IPSC installation?

A. The Microsoft Report Viewer enables embedding reports in applications and supports formatting, printing and exporting of the IPSC security summary and detailed reports.

POLICY

Q. If I use the HP Best Practices Base Policy template and its default settings, will my printing and imaging devices be completely secure?

A. No. The HP Best Practices Base Policy template provides a great place to start when creating a custom policy or when used as a baseline policy. The default settings in this template do not represent complete security for your devices. HP understands that the device security requirements for each customer might differ and offers some of the most common NIST settings as a starting point for developing your custom or baseline policy.

Q. Will any of my third party device solutions be affected by adopting the HP Best Practices Base Policy as is?

A. Possibly. When used with third-party solutions requiring access to the device, the HP Best Practices Policy template might require changes to the default security settings. Refer to your solution documentation to determine whether policy changes are required to accommodate specific functionality. For some third party solutions, the **Command Load & Execute** and **Allow PJL** settings might require enabling.

Q. Should I export my policies?

A. You might export policies for the following reasons:
- To back them up for possible restoration later
- To use for importing into another IPSC server in your corporation

Q. How is my policy information safeguarded when I export the policy?

A. Policies are encrypted when exported. A prompt for a passphrase occurs during the policy export process. This passphrase is required when importing the encrypted policy into IPSC.

Q. How can I easily locate policy configuration settings while accessing the policy editor?

A. From the policy editor, you can use the Enter Search String field for a keyword search. For example, a search for *Apple* displays the *Apple Bonjour* and *Appletalk* setting links. Also use this field to quickly view related technologies for a setting of interest. For example, a search for *Fax* displays *Digital Send*, *Fax PIN*, *Fax Speed Dial Lock*, *Send to Fax* and *User Authentication*. You can also browse categories for specific configuration settings. For example, selecting the Printing category presents the Port 9100, LPD, IPP, WS-Print, FTP, Appletalk, DLC and IPX/SPX printing protocol settings.

Q. Why does a warning icon appear next to one of my policy setting categories after successful validation?

A. A policy can be reviewed and saved as valid with pending policy suggestions. Although not recommended, you can ignore the policy suggestions. For example, if you enable a file system access protocol without enabling the check for a file system access password, this policy is valid, but contains a warning icon next to the policy setting category.

Q. What is the most common reason multiple security policies may be required for my environment?

A. Additional policies are usually required because of variations in the security settings per group of devices. For example, Customer XYZ has grouped their fleet in IPSC by Region A and Region B. Region A would like to implement device credentials that differ from Region B. The recommendation would be to create a Region A and Region B policy that would apply to the respective groups. These policies would be identical, except for the differences in the device credential settings.

DEVICES

Q. At what point in the add devices process is my device actually added to the database?

A. The device is added to the database after you have input an IP address or imported a device list and selected OK. Prior to this, the addresses displayed in the window are not in the database nor do they have a license assigned. You can use this step in the add devices process to clean up a device list before adding to the database and assigning a node license.

Q. What is the value of performing a manual device Verify?

A. You would primarily perform a manual Verify task to confirm the validity of the devices in your list before a device assessment occurs. When IP addresses or hostnames are manually added as devices to IPSC, there is no guarantee that these devices are supported by IPSC or even active on the network. The verify process uses the SNMP and HTTP protocols to gather pertinent device information, such as model name, serial number, firmware versions, credentials, etc. The results of a manual Verify task can become quite useful as criteria for IPSC database cleansing and present IPSC with only a valid list of devices to work with. Although a device Verify automatically occurs behind the scenes as part of a device Assessment, working with a clean database will preserve valuable IPSC performance during assessment related tasks.

Q. I exported a list of devices from HP Web Jetadmin in xml format. Will all the device related information in this file be imported during the add file process?

A. No. IPSC cannot rely on this data being up-to-date, therefore only ip address and hostname information is imported. IPSC then uses DNS to resolve device identification and the Verify process to retrieve additional device information directly from the device. This current device information is then used to populate or update the device tables in the IPSC database.

Q. Why can't I see all of my 2200 devices in the devices window?

A. The devices window displays 1000 devices per page. To see more devices, select **Devices** from the toolbar and advance to the next range of devices.

Q. Why can't I see my filter choices when I right click on the column headings in the devices window?

A. Filters are disabled. Click on the funnel icon in the toolbar. When it changes color to green, filtering is enabled.

Q. Why didn't my node license count increment when I "removed" 10 devices from my custom group after selecting Remove From Group?

A. Even though the devices were removed from your custom group, they are still included in the database, remain part of the **All Devices Group**, and have a license assigned. Only the "deletion" of devices from the **All Devices Group** or any custom group will free up node licenses.

Q. Can IPSC resolve a DNS alias (CNAME), as well as a DNS Hostname?

A. Yes.

Q. I purchased more licenses to accommodate the additional printers I've added. I've loaded the new license file, but licenses are not automatically assigned to these added devices. How do I assign the new licenses?

A. If devices are added to the IPSC database before the license file is loaded, they are set to an unlicensed status. To assign licenses, select the unlicensed devices, right-click and select **License**. You can also select **License** from the **Action** menu or simply **License** from the **All Devices Group**.

Q. I've set an EWS password credential for my All Devices Group, but use a different password credential for 5 high availability printers in this group. How do I set the credentials for these 5 printers in the All Devices Group?

A. Select the 5 devices and right-click for the menu. Select the **Set Credentials** option and set the credentials for the 5 devices.

Q. I've set the appropriate credentials for a custom group of devices. Will new devices that are added to this group inherit the existing credentials?

A. No. Devices added to a group with credentials already set do not inherit that group's credentials. You must manually set credentials on the newly added devices to match the group's credentials.

Q. My device status displays good, but I have a conflicting green check mark and red x icons. Please explain.

A. When viewing devices, there are two separate icon columns to the left of the device status column. The first icon column is referred to as the **Device Status Icon Column**. **Good**, **No Information** and **Error** are the potential status icons found in this column. The left most column is referred to as the **Assessment Status column** and includes the assessment status of **Passed, High Risk**, **Medium Risk**, **Low Risk** or **Not Assessed**. In the scenario above, the device has been verified for good communication and credentials (the green check mark), but assessed with at least one high risk policy setting that is out of compliance (the red x).

ASSESS & REMEDIATE

Q. Why can't I select the Assess and Remediate option in the toolbar of the Policy or Task windows?

A. There is a global device remediation setting found in the File -> Settings -> General window that disables all device remediation. When disabled, **Assess Only** is your only option. Enabling remediation at this global level allows you to select **Assess and Remediate** from the **Policies** and **Tasks** windows.

Q. I have benchmarked the performance of an Assess Only across my fleet of devices. What is the relative performance I can expect when I Assess and Remediate?

A. This depends on how much remediation is required per device, but a good guideline to follow is twice the amount of time of an Assess Only. This is a rough estimate and is based upon every assessed setting being out of compliance with your policy.

Q. Why won't one of my policy settings remediate?

A. Within the policy editor, an individual setting can be configured not to remediate and is most likely the cause. Open the suspect policy and select the setting that is not remediating. Make sure **Advanced Policy Settings** is selected in the view. Now, change the **Remediation** setting from **Disable** to **Enable**. If this is not the issue, then you are experiencing the proper behavior of a setting that, by design, cannot be remediated.

Q. Must I create a new task every time I want to Assess or Assess and Remediate?

A. No. There are several ways to create a new task. You can select a completed task from the **Tasks** window, right click and select **Start**, if it is a task you want to repeat. Or, you can select a completed task, right click and edit the parameters you desire. Or, schedule the task to reoccur at a daily, weekly or monthly interval.

Q. What is the primary value of an Assess Only?

A. Performing an **Assess Only** allows you to validate the comprehensiveness of a newly created policy before remediating any out of compliance devices. **Assess Only** reports security compliance recommendations on each device assessed, which allows you to adjust the policy, if required. Once you are comfortable with your new policy, switching to **Assess and Remediate** keeps your assessed fleet compliant with that policy.

Q. After an assessment, I sometimes see a Device Error in the device recommendations. What does this error indicate?

A. Recommendations are based on the gathering of a device's setting information via an assortment of network protocols and specific ports. If IPSC is unable to gather this information using a specific protocol in the appropriate amount of time, a Device Error is posted for that particular setting.

REPORTS

Q. Why does the Executive Summary Report show an Assessment Risk By Device pie chart with 100% High Risk?

A. This indicates that you have at least one high risk setting out of security policy compliance for every device you assessed.

Q. Does the Executive Summary Report only include Device Summary pie charts?

A. No. The **Executive Summary Report** actually includes three pages of information. Use the page advance at the top of the page to view the additional information. The additional reports are **Assessment Risk (by Devices)**, **Assessment Risk (Policy Items)**, and **Risk Summary**.

Q. On the Risk Summary page of the Executive Summary Report how is the Worst Case Risk total calculated?

A. The policy used in an assessment includes enabled settings with a user assigned severity. The severity choices are high, medium, or low risk. The calculation of Worst Case risk is the total number of "like" severity settings in the policy, multiplied by the number of devices assessed and multiplied again by the specific risk factor multiplier. For example; a policy might have 3 high risk settings and the policy will be used to assess 3 devices. This is a potential for 9 high risk settings to be assessed as out-of-compliance with the policy applied. Utilizing the risk factor multiplier of 10 calculates to be a worst case risk of 90.

Q. Can I save reports?

A. Yes, reports can be saved as a Word or PDF file and archived for historical purposes.

Q. Can I generate a report from a previous period of time?

A. The **Devices Assessed Summary Report** and the **Devices Remediated Summary Report** are the only reports that provide historical data. By executing these reports and selecting an entry from the **Details** or **Last Remediated** column, you will see the policy item, the old value, the new value, time stamp, and the policy used during the assessment and/or remediation.

Q. My reports always provide information for all devices. How can I produce reports on a filtered set of devices?

A. From the **Reports** tab, you can filter devices by selecting a specific group from the **Reports, Executive Summary**, and **Detailed Reports** selections in the left-hand navigation menu. By selecting any of these report options, you will see a **Select Group** option on the toolbar. Use the **Select Group** option to filter devices before generating a report.

Q. Why is the Remediated Summary Report important?

A. Even though IPSC is designed to automatically provide device security assessment and remediation in the background, you might want to know of any remediation patterns that exist in your environment. You might notice a pattern in the Remediated Summary Report that shows a specific device being remediated daily or quite frequently. This pattern would prompt investigation as to why that particular device's security settings are changing and frequently requiring remediation.

INSTANT-ON SECURITY

Q. What is the required IPSC server hostname or DNS alias that enables "automatic" Instant-On functionality?

A. hp-print-mgmt.

Q. Why don't I see the Announcement Agent status on my device's network or security configuration page?

A. Your device might not support this feature yet or may require a firmware upgrade. Please refer to the IPSC Release Notes (www.hp.com/go/ipsc) for details.

Q. Why does my device's network or security configuration page show Announcement Agent failed?

A. This status indicates that the printer did not establish an Instant-On connection with the IPSC server. Probable reasons: The Instant-On feature is not enabled on the IPSC server, TCP Port 3329 is firewall blocked, or the DNS name of hp-print-mgmt is not resolved.

Q. Selecting Mutual Authentication as an Instant-On authentication option nullifies a true out-of-the-box security experience. Why would I use this option for Instant-On?

A. Selecting Mutual Authentication requires the deployment of both device and IPSC certificates for the Instant-On feature to function properly. This manual pre-staging of the device certainly nullifies the initial out-of-box security experience. However, selecting Mutual Authentication provides the most secure interaction for all other Instant-On scenarios. Because certificates remain after a device cold reset, the device can remain somewhat secure until IPSC applies the appropriate security policy.

Q. Does my device always receive the policy configured as the Initial Assessment Policy during an Instant-On scenario?

A. If the device is new to the database or is flagged as "unassessed" in the database, it will receive the Initial Assessment Policy during an Instant-On scenario. If the device is flagged as "assessed" in the database, it will always receive the last policy it was assessed with.

Trademark Credits
Microsoft®, Windows®, Windows Vista®, Windows Server®, and Windows Server System® are U.S. registered trademarks of Microsoft Corporation.

© 2013 Copyright Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an

c02700115ENW, Rev. 2, December 2013